Incident Post Mortem: 2 RO Credential Phish

Issue Summary

- An RO's credentials (network login name and password) were phished (stolen on the internet).

Timeline

- Issue reported and dealt with on August 13, 2015
- 16 (2) (c)

Root Cause

- 16 (2) (c)
-

Resolution and recovery

- The user's password was reset immediately and investigation started. No evidence that a breach has occurred was found.

Corrective and Preventative Measures

- Increase awareness and 16 (2) (c),21 (1) (a)
- Continue the phishing campaign

Incident Post Mortem: 4 RO Phish #2

Issue Summary

- The ROTC were notified by the AC in ED 48015 that they had fallen victim to a phishing attack. The VM was immediately shut down and it was determined that suspicious activities had occurred. The VM was purged, all system were scanned with our security software, 16 (2) (c) 16 (2) (c) and we re-installed the Guest image from the nightly back-up with the assistance from our colleagues in ITAS.

Timeline

- Issue reported August 17, 2015

Root Cause

- 16 (2) (c)

Resolution and recovery

- Investigation found that the AC had brought their home laptop, plugged it into the ROTC network, then opened their personal webmail, then clicked on a phishing site. With the machine being wiped clean it was difficult to perform more analysis of what happened, but on the network we are all clear.

Corrective and Preventative Measures

- Increase awareness and 16 (2) (c).21 (1) (a)

Incident Post Mortem: 5 Suspicious Employee

Issue Summary

- An employee who had been dismissed had been acting "suspicious" by insisting on taking his all-in-one computer with him when he was moved from cubicle to cubicle. After he was dismissed it was decided to investigate.

Timeline

- August 18, 2015 issue was reported to ITSec team

Root Cause

- 16 (2) (c) [redacted]

Resolution and recovery

- First findings found a VM had been installed, and several pieces of software and media were downloaded (many illegally) and most likely installed on this VM. No media downloads seemed to indicate they were illegal other than copyright infringement. Unable to get into VM without more work. It was decided to end the investigation at that point.

Corrective and Preventative Measures

- Increase awareness and 16 (2) (c).21 (1) (a) [redacted]

Incident Post Mortem: 6 DropBox issue

Issue Summary

- On August 17th 2015, EC system 16 (2) (c),19 (1) transferred 16 (2) (c) of information to Dropbox between 2:08:51 PM and 2:18:55 PM. The user was contacted and confirmed that it was EC data. The user was contacted and asked to delete the information and discontinue use of Dropbox.

Timeline

- Issue detected by 16 (2) (c) on August 18, 2015
- 16 (2) (c)

Root Cause

- 16 (2) (c)

Resolution and recovery

- 16 (2) (c)

Corrective and Preventative Measures

- Awareness and 16 (2) (c),21 (1) (a)
- 16 (2) (c)

Incident Post Mortem: 10 SQL Injection at Bell

Issue Summary

- Someone posted on Reddit that they successfully performed SQL Injection on an EC production application, which was then tweeted on twitter. They claimed they had reported it to EC (meaning Bell) and that someone had fixed it. Contract App

Timeline

- Issue reported September 9, 2015.

Root Cause

- 16 (2) (c) [redacted]

Resolution and recovery

- Investigation found that the SQL injection did happen, although the information gained was not sensitive. The vulnerable application has been removed and the remaining similar application has had a patch applied 16 (2) (c) [redacted]
16 (2) (c) [redacted]

Corrective and Preventative Measures

- 16 (2) (c),21 (1) (a) [redacted]

Incident Post Mortem: 13 LiveRail.com

Issue Summary

- 16 (2) (c) alerted the ITSec team that senior individuals in our organization were uploading large amounts of data to an external site without their knowledge. Some of the data was encrypted, and it had gone on at least 7 days and over 600 employees were affected by this situation.

Timeline

- Issue was picked up by 16 (2) (c) on September 11, 2015.

Root Cause

- Click-fraud/aggressive online advertising.

Resolution and recovery

- This issue was escalated almost immediately to GC CIRT, who responded by sending someone to collect and analyze data 16 (2) (c) After much analysis from GC CIRT, 16 (2) (c) and the EC ITSec team it was determined that this was not malware, it was just click fraud (a website creating fake traffic, for profit, at the expense of our bandwidth). During the investigation internet access was shut down to the 10th floor to protect the register and the URL in question was blocked, as well as facebook.

Corrective and Preventative Measures

- LiveRail.com and all other similar style websites are now blocked
- Department-wide ad blocking is being rolled out, via an intake.

Incident Post Mortem: 16 LogMeIn

Issue Summary

- Several machines have visited and used logmein.com and other types of services that allow users to control their machine from home, passing through this external website. This does not follow our Acceptable Use Policy and also presents a possible security risk.

Timeline

- 16 (2) (c) picked up the activity on September 29, 2015

Root Cause

16 (2) (c)

Resolution and recovery

- LogMeIn.com and some other sites similar to it were blocked.

Corrective and Preventative Measures

- Increase IT security awareness , including the AUP and ITSec policies
- 16 (2) (c),21 (1) (a)

Incident Post Mortem: 29 IIS Logs Oct 13, Oct 14

Issue Summary

- 16 (2) (c) The applications in question contained only non-sensitive data, and no data was changed on the server(s).

Timeline

- October 13, 2015 – SQL injection attack attempts discussed with 16 (2) (c)
- October 14, 2015 – SQL injection attack attempts discussed with 16 (2) (c) 16 (2) (c)
- October 15, 2015 – As there was no way to securely transfer such large files, 16 (2) (c) picked up the files in person
- 16 (2) (c)
-

Root Cause

16 (2) (c)

Resolution and recovery

- We removed the applications from internet before polling day (October 19, 2015).

Corrective and Preventative Measures

16 (2) (c).21 (1) (a)

Incident Post Mortem: 32 CE15-1016-04 Special Report

Issue Summary

- A report was received from 16 (2) (c) that 3 EC public-facing web applications had had successful SQL injection attempts.
- 2 of the 3 apps had already been reported on previously.
- All 3 apps contained only non-sensitive data
- No data was changed on the server(s)

Timeline

- Report received October 19th, 2015
- Investigation and reporting completed by October 20, 2015

Root Cause

- 16 (2) (c)

Resolution and recovery

- We removed the applications from internet before polling day (October 19, 2015).

Corrective and Preventative Measures

- 16 (2) (c),21 (1) (a)

Incident Post Mortem: 33 CE15-1019-23 ELETC Special Report

Issue Summary

- A java/flash malware was reported to have been downloaded on the EC network, several times.
- 32 people verified as affected

Timeline

- Issue reported October 19, 2015 (polling day)
- Investigation and notifications complete by October 20, 2015

Root Cause

- 16 (2) (c)

Resolution and recovery

- All users who were possibly affected were notified and asked to change all of their web passwords, work and personal. We also changed several passwords for web applications that we felt might have been affected, and blocked all sites listed in the report.

Corrective and Preventative Measures

- 16 (2) (c),21 (1) (a)
-

Incident Post Mortem: 34 Malware detected pop up can't close ID: 525633

Issue Summary

- AC Clicked on malicious link accidentally, was infected with Malware.

Timeline

- Monday October 19, 2015, incident reported, investigated and actioned

Root Cause

- 16 (2) (c) [redacted]

Resolution and recovery

- Machine quarantined, and wiped. Network and business server not affected.

Corrective and Preventative Measures

- 16 (2) (c),21 (1) (a) [redacted]
- [redacted]

Incident Post Mortem: 38 Virus-malware at 59037 - AARO3 HV ticket 523179 Lenovo

Issue Summary • An employee from an AARO office clicked on a phishing link and their machine was believed to be infected with malware.
Timeline • October 18, 2015
Root Cause • Phishing is common.
Resolution and recovery • The machine was removed from the network, the user's password was reset. No damage done.
Corrective and Preventative Measures • 16 (2) (c),21 (1) (a)

Sommaire d'incidents enquêtés

Élection Canada 2014 - (16 juin) 2017

2014 (1 incident)

Date	Description	Report Available?
22-Dec-14	Activité suspecte	N

2015 (21 incidents)

Date	Description	Report Available?
01-Jan-15	Activité suspecte	N
13-Aug-15	Hameçonnage	Y (2)
17-Aug-15	Hameçonnage	Y (4)
18-Aug-15	Activité suspecte	Y (5)
18-Aug-15	Activité suspecte	Y (6)
24-Aug-15	Vol d'équipement	Y (36)
30-Aug-15	Vol d'équipement	Y (8)
03-Sep-15	Perte d'équipement	Y (9)
09-Sep-15	Activité suspecte	Y (10)
10-Sep-15	Vol d'équipement	Y (12)
11-Sep-15	Activité suspecte	Y (13)

Date	Description	Report Available?
16-Sep-15	Vol d'équipement	Y (15)
29-Sep-15	Activité suspecte	Y (16)
06-Oct-15	Activité suspecte	Y (20)
13-Oct-15	Activité suspecte	Y (29)
15-Oct-15	Activité suspecte	Y (25)
18-Oct-15	Maliciel	Y (38)
19-Oct-15	Activité suspecte	Y (32)
19-Oct-15	Maliciel	Y (33)
19-Oct-15	Maliciel	Y (34)
24-Dec-15	Activité suspecte	Y (A)

2016 (0 incident)

Nul

2017 (0 incident)

Nul

IIS servers log from the web front end servers were reviewed from December 1st to December 27th. Logs were parsed via a tool with SQL keyword (e.g. SELECT, CAST, DECLARE etc…)
Parsing results displayed SQL Code injections which had been passed from the IIS web server to the SQL Server.
The results indicate that the attacker gained access through the 16 (2) (c) on Dec 24th, 2015.

Suspicious activity prior to and including Dec 24th

16 (2) (c),19 (1) - active Dec 2; targeting multiple pages, but not
16 (2) (c),19 (1) - active Dec 13; targeting 16 (2) (c)
16 (2) (c),19 (1) - active Dec 17; targeting 16 (2) (c)
16 (2) (c),19 (1) active Dec 17 and 24; targeting
- active Dec 22; targeting 16 (2) (c)
16 (2) (c),19 (1) – active Dec 24; targeting 16 (2) (c)

Dec 24th:
Logs indicate that the attacker [operating using at least 16 (2) (c),19 (1) gained access through the 16 (2) (c) . This may have been reconnaissance for a later exfiltration. Teams at EC, 16 (2) (c) are working to prove the time and content but suspected traffic can be seen from 23:32 GMT

Dec 26th:
Pastebin created claiming to be a sample of compromised data.

Dec 27th:
Reddit thread with link to Pastebin sample of compromised data, and a copy of the same data on 0bin

At 8:53pm **CE15-1227-01 ELECTC Possible Data Disclosure** message sent to member of the EC IT Security staff

Dec 28th:
At 10am EC CIO reaches out to member of the EC IT Sec team indicating that SSC is looking to discuss possible incident.

SSC provides link to Pastebin. EC is able to confirm information is genuine. 16 (2) (c)
16 (2) (c)

Dec 29th:
16 (2) (c) conference call at 1pm (followed by shortened day due to conditions)
identified the table 16 (2) (c) were compromised, 16 (2) (c) to backup then remove the following tables:
16 (2) (c)

16 (2) (c)

DAS Lead 16 (2) (c),19 (1) engaged to assign DAS team to review server and dbase logs. (Dec 26/27th target dates)

SOC 16 (2) (c),19 (1) assessing all 16 (2) (c) HIPS/NIPS logs for SQL injections. (Target Dec 26 and Dec 27th).

16 (2) (c)

Dec 30th:

16 (2) (c)

Confirmation was also received from NHS that the SQL Servers are not accessible via internet. This provides further validation that the vulnerability was a SQL injection.

Implemented the following activities to contain the threat **(Mtce page posted at 6:00 pm with user/password and dbases disabled by 7:30 pm) :**

- 16 (2) (c)
- Post a maintenance page for the impacted applications.
  16 (2) (c)
- 16 (2) (c)
- This is intended to be in place temporarily until Monday Jan 4th when the 16 (2) /EC teams can regroup to review the MOP for the proposed changes to the user account/password.
- Web Server/FW/HIP logs to be sent to 16 (2) (c) at EC. (target dates Dec 26/27th) Files were posted on FTP morning of Dec 31st.
- Monday Jan 4th, conference call will be scheduled betwee 16 (2) /EC primes (EC to confirm names) to discuss the plan and impacts to the applications. 16 (2) (c)

16 (2) (c)

- 16 (2) (c) confirmed that the 16 (2) (c) Clean up process will be coordinated with MS web on Monday Jan 4th
- 16 (2) (c)
- The investigation to determine the entry point for the hacking is still under investigation, we are in the process of reviewing all server logs and SOC team are also doing a deep dive for any suspect behavior that might require a new signature. More details will be forthcoming as this part of the investigation continues real time.

Jan 4th:

Conference call at 11:00 am between 16 (2) /EC team to review next steps. Phil Hopkins now engaged to review the issue. Action items include:

- 16 (2) expanded the IIS/Http Error log review to include (Dec 25 –Dec 1st) Working backwards. – 16 (2) (c),19 (1)
- Copy the IIS+HTTPERR logs ranging from dec 20th until dec 27th, from all the 16 (2) (c) Web servers, on to the FTP server – 16 (2) (c),19 (1)
- 16 (2) (c),19 (1) will provide additional key words t 16 (2) (c),19 (to assist in the review. – Prime
- EC Security will provide the VA in a new format to SOC team. – 16 (2) (c)
- MS Web will provide a complete list of all script folders – 16 (2) (c)
- Prior to any cleanup activities, MS web will perform a complete back up of the SQL server – 16 (2) (c)
- EC will review the application code leveraging the SQL servers – 16 (2) (c)
- A copy of the backup will be zipped and sent to EC. – 16 (2) (c),19 (1)
- EC will review all data with their teams to ensure what data/apps can be deleted. That will also determine the apps that will remain and will be impacted by the User/Password change. – 16 (2) (c)
- A final list of URL's that will use the User/Password (as well as a list of exactly the changes are required) to be provided for the implementation plan. 16 (2) (c)
- Implementation plan/dates to be determined based on instruction from EC (including any possible code change required to support hashing) – 16 (2) (c)

Decision: 16 (2) (c)

Jan 5th:

16 (confirmed that on Dec 24th the investigation indicates that the attacker gained access through the 16 (2) (c)

- A copy of ALL dbases on the SQL server were sent to EC
- Complaint form schema and Moodle Schema posted in same FTP Folder.
- Globally – 16 (to provide all details on that source IP, everywhere that it tried to access.
- EC now in "assessment" phase of the data to better determine their exposure due to this SQL Injection.
- Confirmed that all SQL dbases will remain offline and 16 (2) (c)